```
Input: $M, n, e = (e_{w-1} \cdots e_2 e_1 e_0)$
Ouput: $S = M^e \bmod n$

Let $S = 1$
FOR $k = w-1$ downto 0
    $S = (S \cdot S) \bmod n$
    IF ($e_k$ is 1 ) THEN
        $S = (S \cdot M) \bmod n$
    ENDIF
ENDFOR
RETURN S
```

FIG.1(Prior Art)

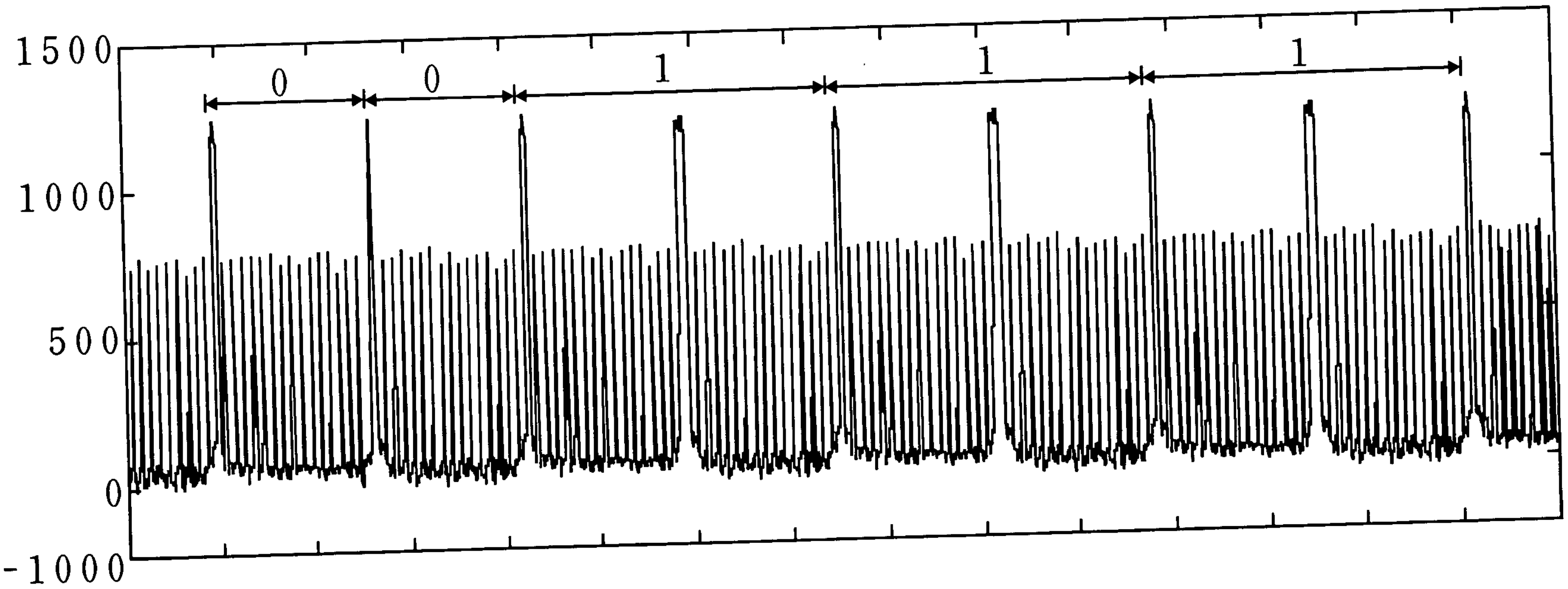


FIG.2(Prior Art)

Input: M, n, $e = (e_{w-1}\cdots e2e1e0)$

Ouput: $S = M^{e} \bmod n$

```
Let $S_0 = 1; S_2 = M$
FOR $k = w-1$ downto 0
    $b = \sim e_k$
    $S_0 = (S_0 \cdot S_0) \bmod n$
    $S_b = (S_2 \cdot S_b) \bmod n$
ENDFOR
RETURN $S_0$
```

FIG.3(Prior Art)

Input: M, n, $e = (e_{w-1}\cdots e_2e_1e_0)$

Ouput: $S_0 = M^{e} \bmod n$

Algorithm : assume $e_{w-1}=1$

```
$e_{-1}=1$
$S_0 = 1$ ;  $S_1 = M$
FOR $k = w-1$ downto 0 DO
    $b = \sim e_k$ ; $c = e_{k-1}$
    $S_0 = (S_0 \cdot S_b) \bmod n$; $S_0 = (S_0 \cdot S_c) \bmod n$
ENDFOR
RETURN $S_0$
```

FIG.4

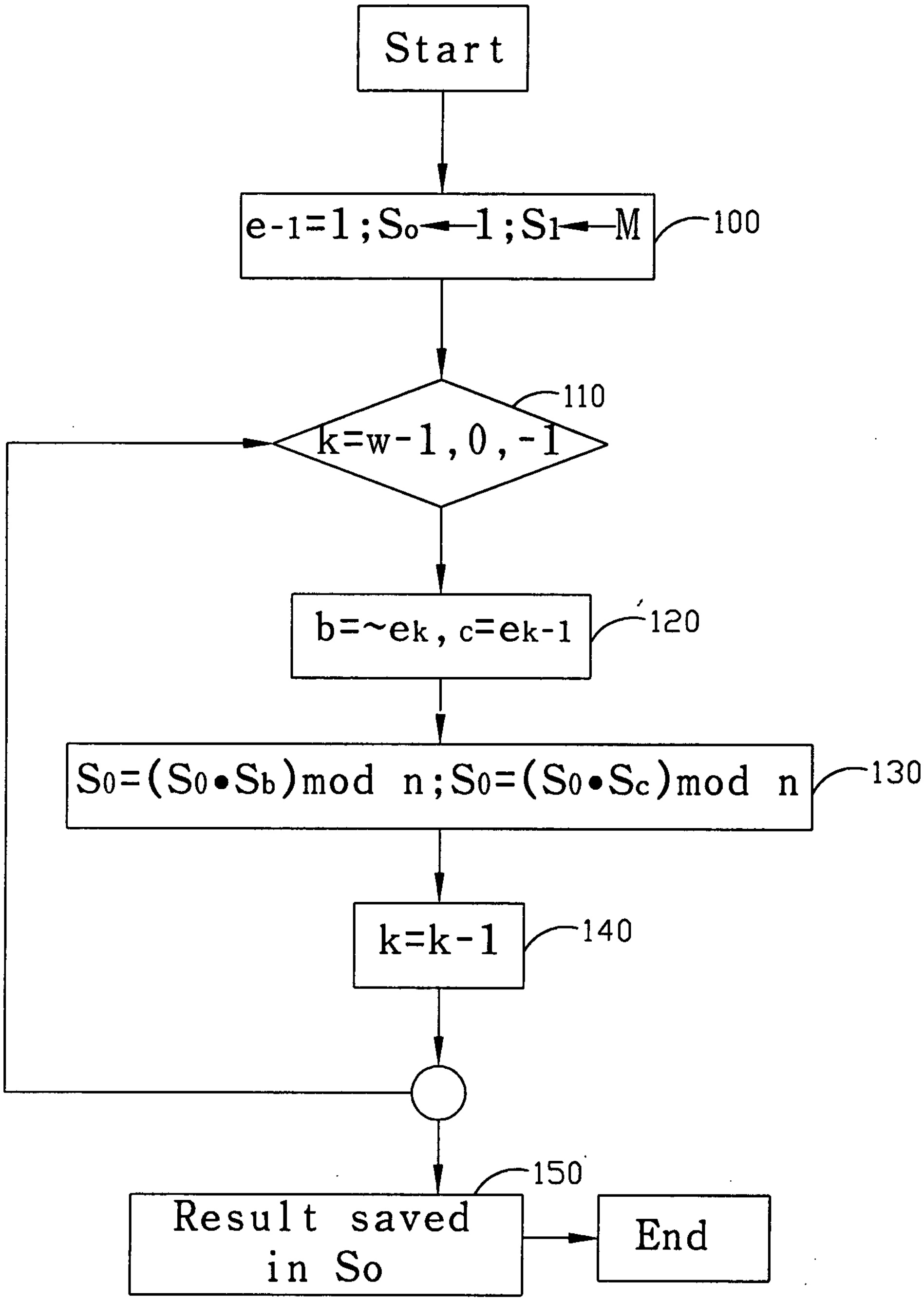
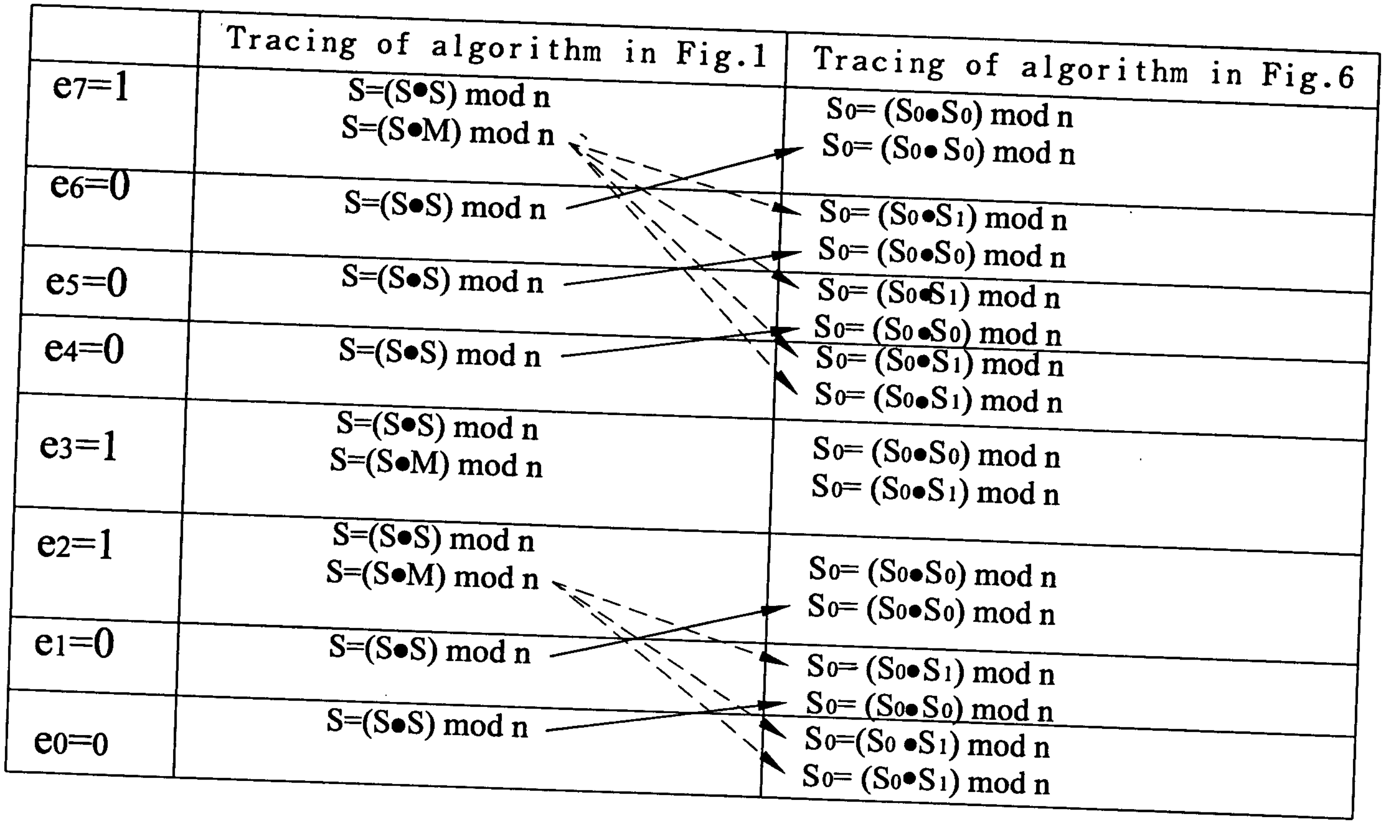

Start
$e_{-1}=1; S_o \leftarrow 1; S_1 \leftarrow M$
100
$k=w-1,0,-1$
110
$b=\sim e_k, c=e_{k-1}$
120
$S_0=(S_0 \bullet S_b) \bmod n; S_0=(S_0 \bullet S_c) \bmod n$
130
$k=k-1$
140
150
Result saved in So
End

FIG.5



	Tracing of algorithm in Fig.1	Tracing of algorithm in Fig.6

e7=1	S=(S•S) mod n
	S=(S•M) mod n
		S_0= (S_0•S_0) mod n
		S_0= (S_0• S_0) mod n

e6=0	S=(S•S) mod n	S_0= (S_0•S_1) mod n S_0= (S_0•S_0) mod n
e5=0	S=(S•S) mod n	S_0= (S_0•S_1) mod n S_0= (S_0•S_0) mod n
e4=0	S=(S•S) mod n	S_0= (S_0•S_1) mod n S_0= (S_0•S_1) mod n

e3=1	S=(S•S) mod n
	S=(S•M) mod n
		S_0= (S_0•S_0) mod n
		S_0= (S_0•S_1) mod n

e2=1	S=(S•S) mod n
	S=(S•M) mod n
		S_0= (S_0•S_0) mod n
		S_0= (S_0•S_0) mod n

e1=0	S=(S•S) mod n	S_0= (S_0•S_1) mod n S_0= (S_0•S_0) mod n
e0=0	S=(S•S) mod n	S_0=(S_0 •S_1) mod n S_0= (S_0•S_1) mod n

FIG.6